Document made available under the Patent Cooperation Treaty (PCT)

International application number: PCT/US04/019917

International filing date: 21 June 2004 (21.06.2004)

Document type: Certified copy of priority document

Document details: Country/Office: US
Number: 60/519,792
Filing date: 13 November 2003 (13.11.2003)

Date of receipt at the International Bureau: 27 August 2004 (27.08.2004)

Remark: Priority document submitted or transmitted to the International Bureau in compliance with Rule 17.1(a) or (b)

World Intellectual Property Organization (WIPO) - Geneva, Switzerland
Organisation Mondiale de la Propriété Intellectuelle (OMPI) - Genève, Suisse

1212928

THE UNITED STATES OF AMERICA

TO ALL TO WHOM THESE PRESENTS SHALL COME:

UNITED STATES DEPARTMENT OF COMMERCE

United States Patent and Trademark Office

August 17, 2004

THIS IS TO CERTIFY THAT ANNEXED HERETO IS A TRUE COPY FROM THE RECORDS OF THE UNITED STATES PATENT AND TRADEMARK OFFICE OF THOSE PAPERS OF THE BELOW IDENTIFIED PATENT APPLICATION THAT MET THE REQUIREMENTS TO BE GRANTED A FILING DATE.

APPLICATION NUMBER: *60/519,792*
FILING DATE: *November 13, 2003*
RELATED PCT APPLICATION NUMBER: *PCT/US04/19917*

Certified by

Jon W Dudas

Acting Under Secretary of Commerce
for Intellectual Property
and Acting Director of the U.S.
Patent and Trademark Office

11696 U.S. PTO

HAMILTON, BROOK, SMITH & REYNOLDS, P.C.

PROVISIONAL APPLICATION FOR PATENT COVER SHEET

This is a request for filing a PROVISIONAL APPLICATION FOR PATENT under 37 C.F.R. 1.53(c)

22387 U.S. PTO
60/519792
111303

Express Mail Label Number EV 005371167 US

Docket Number 3174.1012-001

INVENTOR(S)		
Given Name (first and middle (if any))	Family Name or Surname	Residence (Street Address, city and either state or Foreign Country)
David A.	Waldman	Concord, MA
[X] Additional inventors are being named on the separately numbered sheet(s) attached hereto		

TITLE OF THE INVENTION (500 characters max)

METHOD FOR HIGH RESOLUTION FINGERPRINT CAPTURE AND IDENTIFICATION

CORRESPONDENCE ADDRESS

Direct all correspondence to:

NAME	Customer No. 021005				
	HAMILTON, BROOK, SMITH & REYNOLDS, P.C.				
ADDRESS	530 Virginia Road, P.O. Box 9133				
CITY	Concord	STATE	MA	ZIP CODE	01742-9133
COUNTRY	USA	TELEPHONE	(978) 341-0036	FAX	(978) 341-0136

ENCLOSED APPLICATION PARTS ***(check all that apply)***

[X] Specification *Number of Pages* [15]

[X] Drawing(s) *Number of Sheets* (interspersed throughout text)

[ ] Other (specify) ____________

METHOD OF PAYMENT OF FILING FEES FOR THIS PROVISIONAL APPLICATION FOR PATENT (check one)

[X] A check or money order is enclosed to cover the filing fees. Please charge any deficiency in fees and credit any overpayment to Deposit Account Number 08-0380.

[ ] The Director is hereby authorized to charge filing fees or credit any overpayment to Deposit Account Number 08-0380.

FILING FEE AMOUNT ($)

$160

The invention was made by an agency of the United States Government or under a contract with an agency of the United States Government.

[X] No

[ ] Yes, the name of the U.S. Government agency and the Government contract number are: ____________

Signature	*[signature]*	Date	11/13/03
Submitted by Typed or Printed Name	Timothy J. Meagher	Reg. Number	39,302

Rev. August 4, 1999

PROVISIONAL APPLICATION COVER SHEET
Additional Page

Docket Number	3174.1012-001

INVENTORS		
Given Name (first and middle (if any))	Family Name or Surname	Residence (Street Address, city and either state or Foreign Country)
Vincent	Fedele	Harvard, MA
Richard T.	Ingwall	Newton, MA
John S.	Berg	Franklin, MA
David L.	Kent	Framingham, MA
Joby	Joseph	Waltham, MA

@PFDesktop\::ODMA/MHODMA/IMANAGE;433717;1

Express Mail Label No. EV005371167US
Date: 11/13/03
IManage 433466

Method for High Resolution Fingerprint Capture and Identification

Field of the Invention

This invention relates to the field of automatic fingerprint image analysis, and includes the steps of fingerprint acquisition, fingerprint enrollment and fingerprint identification. It applies, in particular, to the automatic analysis of high resolution fingerprint images that reveal pore structural features and ridge deviation details in addition to standard minutiae structures.

Background of the Invention

Growing concerns regarding domestic security have created a critical need to positively identify individuals as legitimate holders of credit cards, driver's licenses, passports and other forms of identification. The ideal identification process is reliable, fast, and relatively inexpensive. It should be based on modern high-speed electronic devices that can be networked to enable fast and effective sharing of information. It should also be compact, portable, and robust for convenient use in a variety of environments, including airport security stations, customs and border crossings, police vehicles, home and office computing and entrance control sites of secure buildings.

A well established method for identification is to compare a fingerprint with a previously obtained authentic fingerprint of the individual (Maltoni, Maio, Jain, and Prabhakar, "Handbook of Fingerprint Recognition", Springer, 2003, chapter 1). Fingerprints have traditionally been collected by rolling an inked finger on a white paper. Since this traditional process clearly fails to meet the criteria listed above, numerous attempts have been made to develop an electronically imaged fingerprint method to address new security demands. These modern methods all use, as a key component, a solid-state device such as a capacitive or optical sensor to capture the fingerprint image in a digital format. By using a solid-state imager as part of a fingerprint identification apparatus a fingerprint can be collected conveniently and rapidly during a security check, for example, and subsequently correlated, in near real-time, to previously trained digital fingerprints in an electronic data base. The data base can reside on a computer at the security check point, on a secure but portable or removable storage device, on a remotely networked server, or as a biometric key embedded into a smartcard, passport, license, birth certificate, or other form of identification.

The topological features of a typical finger comprise a pattern of ridges separated by valleys, and a series of pores located along the ridges. The ridges are 100 to 300 μm wide and can extend in a swirl-like pattern for several mm to one or more cm. The ridges are separated by valleys with a typical ridge-valley period of approximately 250-500 μm. Pores, roughly circular in cross section, range in diameter from about 50 μm to 250 μm, and are aligned along the ridges. The patterns of both ridges/valleys and pores are believed to be unique to each fingerprint. No currently available commercial fingerprint acquisition technique is able to resolve pores. Accordingly present-day automatic fingerprint identification procedures use only ridge and valley patterns. There are particular patterns of ridges, called minutiae, such as ridge end-points, deltoids, bifurcations, crossover points, and islands, which are found in almost every fingerprint

(Maltoni, Maio, Jain, and Prabhakar, "Handbook of Fingerprint Recognition", Springer, 2003, chapter 3) Extraction and comparison of minutiae is the basis of most current automatic fingerprint analysis systems.

There are several important limitations with minutiae-based methods of automatic fingerprint analysis. In order to collect enough minutiae for reliable analysis a relatively large, at least 0.50 x 0.50 inches, good quality, fingerprint, or latent image of a fingerprint must be available. Large prints are often collected by rolling an inked finger on a white card, and subsequently scanning the inked image into an electronic data base. This manual procedure is an awkward and time consuming process that requires the assistance of a trained technician. Automated methods for collecting large fingerprints usually require mechanically complicated and expensive acquisition devices. Large area fingerprints suffer from distortions produced by elastic deformations of the skin so that the geometrical arrangements between minutiae points vary from image to image of the same finger. In addition, forensic applications can involve small, poor quality latent prints that contain relatively few resolved minutiae so that reliable analysis based on a limited number of minutiae points is quite difficult.

Minutiae comparison ignores a significant amount of structural information that could be used to enhance fingerprint analysis. Since the typical fingerprint contains between 7 to 10 times as many pores as minutiae, techniques that include both pores and minutiae should greatly improve matching compared to techniques that use only minutiae. Stosz and Alyea (J. D. Stosz, L. A. Alyea, "Automated system for fingerprint authentication using pores and ridge structures", Proc. SPIE, vol 2277, 210-223, 1994) have confirmed this expectation by showing that the use of pores combined with minutiae improves the accuracy of fingerprint matching, and allows successful analysis of relatively small prints. Their image sensor used a common prism-based configuration, a high resolution CCD video camera, and a macro lens to provide the resolution needed to image pores. After acquisition the gray-scale images are converted to a binary format and then processed further to produce a skeleton image from which minutiae and pores are identified. Fingerprints are compared by independent correlations between pores and minutiae extracted from the various images.

Summary of the Invention

Although the procedure of Stosz and Alyea is useful for high resolution images, it does not improve the analysis of the very large number of previously acquired, lower resolution fingerprints that do not have resolved pores. Their process, which converts ridges to contour lines through binarization and thinning, also discards information regarding ridge shape that could be used to aid fingerprint matching(see Figure 4).

There is a need, therefore, for a procedure that improves the analysis of both high resolution fingerprints that contain pores, and lower resolution fingerprints without resolved pores. Our procedure fulfills this need by using identifying information in a fingerprint that can include ridge shapes or profiles in addition the usual ridge contours, and the position, shape and prominence of pores.

Our procedure is an automatic fingerprint recognition method that identifies fingerprint features by using gray-scale gradient edge detection techniques. The techniques identify and trace edges of structural features to outline ridges and pores. At sufficiently high resolution the ridge outlines contain structural features that can be used

in fingerprint matching. This capability improves matching reliability over systems that reduce ridge patterns to a few minutiae types, or consider ridges only as simple contour lines. Because of the richness of features in fingerprints at high resolution our procedure produces reliable matching of small prints. The procedure analyzes an unaltered gray-scale image of the fingerprint to reduce both computing time and false accept rates. In a preferred embodiment edge detection software is combined with high resolution image acquisition technology that is capable of resolving pores and ridge profiles.

Description of the Invention

The invention comprises two major steps; fingerprint enrollment and fingerprint matching. During enrollment a high resolution digital fingerprint is acquired and features of the resulting image that will be used for subsequent fingerprint matching are identified. Fingerprint matching compares features from two fingerprints and decides if the two prints are from the same individual. The source for these two prints can be a data base of high resolution fingerprints, a live scan image, a legacy data base of lower resolution prints, or latent fingerprints, or combinations of these sources.

Fingerprint Enrollment

A block diagram of the fingerprint enrollment process is presented in Figure 1. Fingerprint matching is described latter in the application.

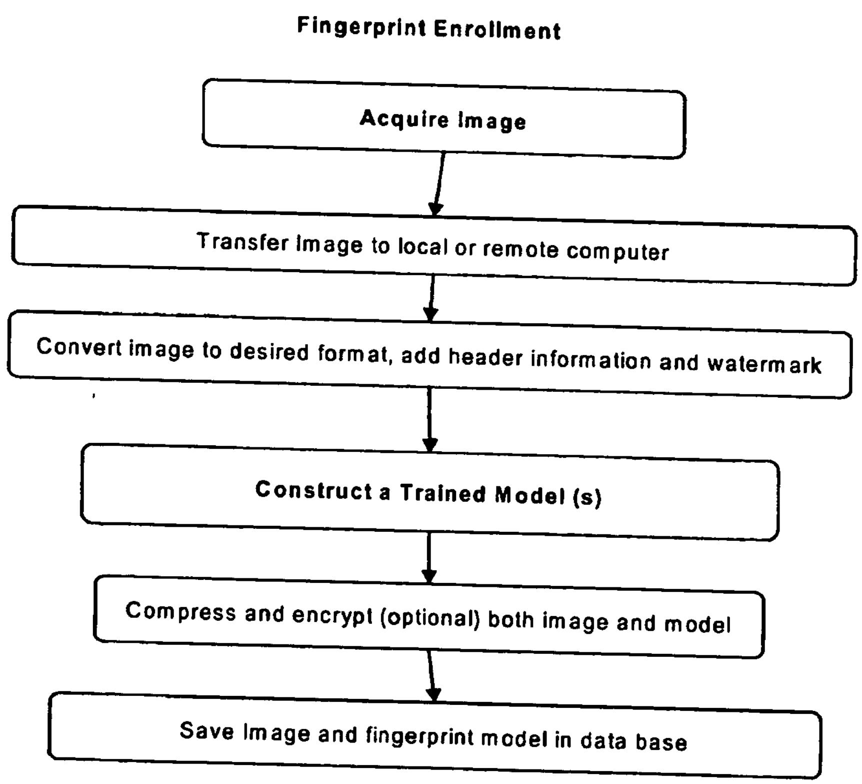

Figure 1. A flow diagram of the enrollment step of the invention:. The blocks in bold type are further broken down in additional flow diagrams in Figures 3 and 4.

Fingerprint Acquisition:

Although our procedure can improve the analysis of low resolution fingerprints it is particularly useful for the analysis of high resolution images that show pores as well as ridge features. There are many ways to detect a fingerprint, (Maltoni, Maio, Jain, and Prabhakar, chapter 2). Our preferred method of acquiring high resolution fingerprints is outlined in Figure 3, and described more fully in the US patent application 60/480,008, filed June 21, 2003, which is incorporated by reference herein in its entirety. This method uses the device shown in Figure 2.

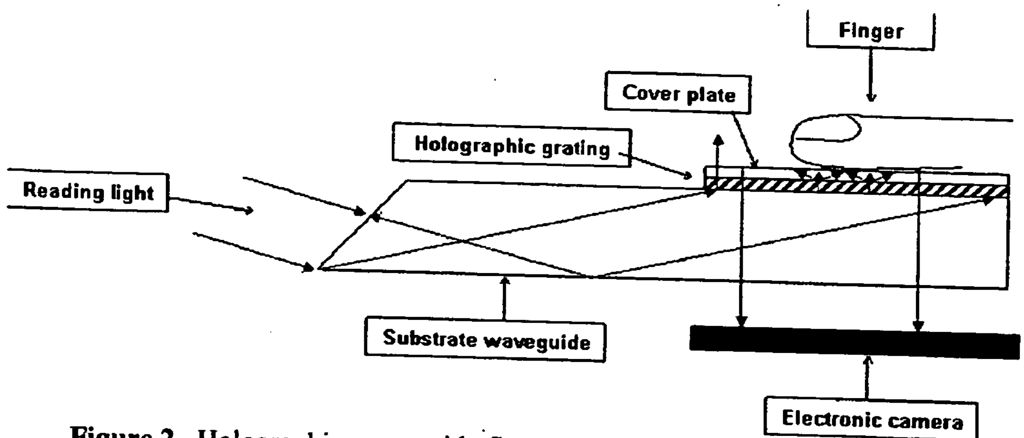

Figure 2. Holographic waveguide fingerprint imager

The key components of the image acquisition device of Figure 2 are a reading light source, a substrate that acts as a waveguide for the read light, a holographic grating, a cover plate, and an electronic camera. Reading light, usually from a low-power diode laser, is directed onto the entrance face of the substrate waveguide at an angle that causes the light to be guided through the substrate by total internal reflection at the substrate-air interfaces. The guided light beam is diffracted from the guide at a near normal angle to the guide surface by the holographic grating. Fresnel reflection of the diffracted light at the coverplate directs some of the diffracted light back through the hologram, through the substrate waveguide, and onto the entrance face of the electronic camera. Reflection at the cover plate is suppressed at locations where objects come into optical contact with the plate. The remaining reflected light will carry an image of these contact areas to the electronic camera.

When a finger is pressed onto the cover plate the ridges of the fingerprint will make optical contact and suppress reflection. Since pores are depressions along the ridges there will be reflection from the coverplate at pore locations. The resulting image of the finger that is presented to the digital camera comprises light areas for the valleys, and dark ridges with light pores aligned along the ridges. An undistorted, high resolution image of the fingerprint can be captured by the camera if the reading light that is diffracted by the hologram is collimated and has a uniform wavefront.

A specific example of the device shown in Figure 2 that has been used in our laboratory to successfully acquire high resolution fingerprints uses a laser diode that emits 5 mW of light at 652nm. The glass waveguide has an entrance face for the laser

light that is beveled to an angle of 60 degrees from the horizontal; its dimensions are 36 mm long, 2.5 mm thick and 25 mm wide; the 1 mm thick square coverplate is 25 x 25 mm. In this example the image is captured by a CMOS electronic imager having a 1024 by 1280 array of 6μm square pixels and 256 gray levels. The size of the resulting image is 6.1 mm by 7.7 mm, while its resolution is 167 pixel per mm or 4200 pixels per inch.

An example of a high resolution fingerprint that was acquired with the device described above according to the method of Figures 2 and 3 is shown in Figure 4. The light valleys and dark ridges with their associated bright pores are easily resolved. Examples of pores, ridges, ridge details, and minutiae are all indicated in the figure. Some or all of these types of features can be used by our procedure to compare and match fingerprint images.

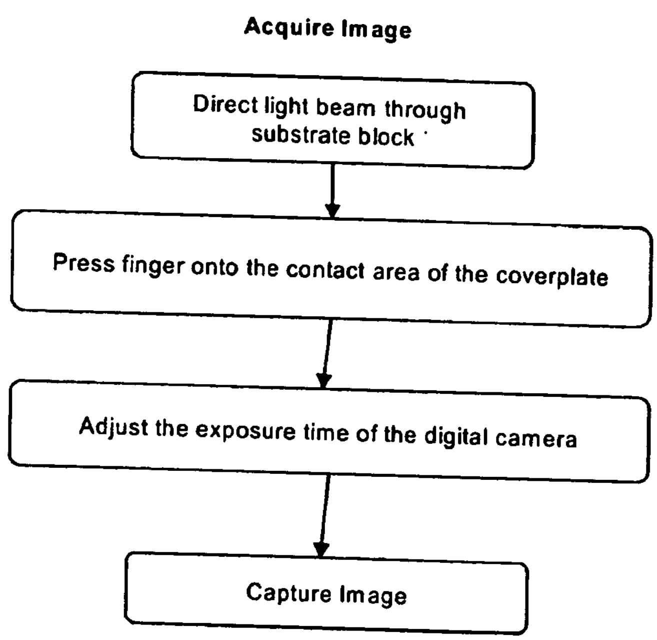

Figure 3. A flow diagram for the acquisition of a fingerprint with resolved pores ridge profiles.

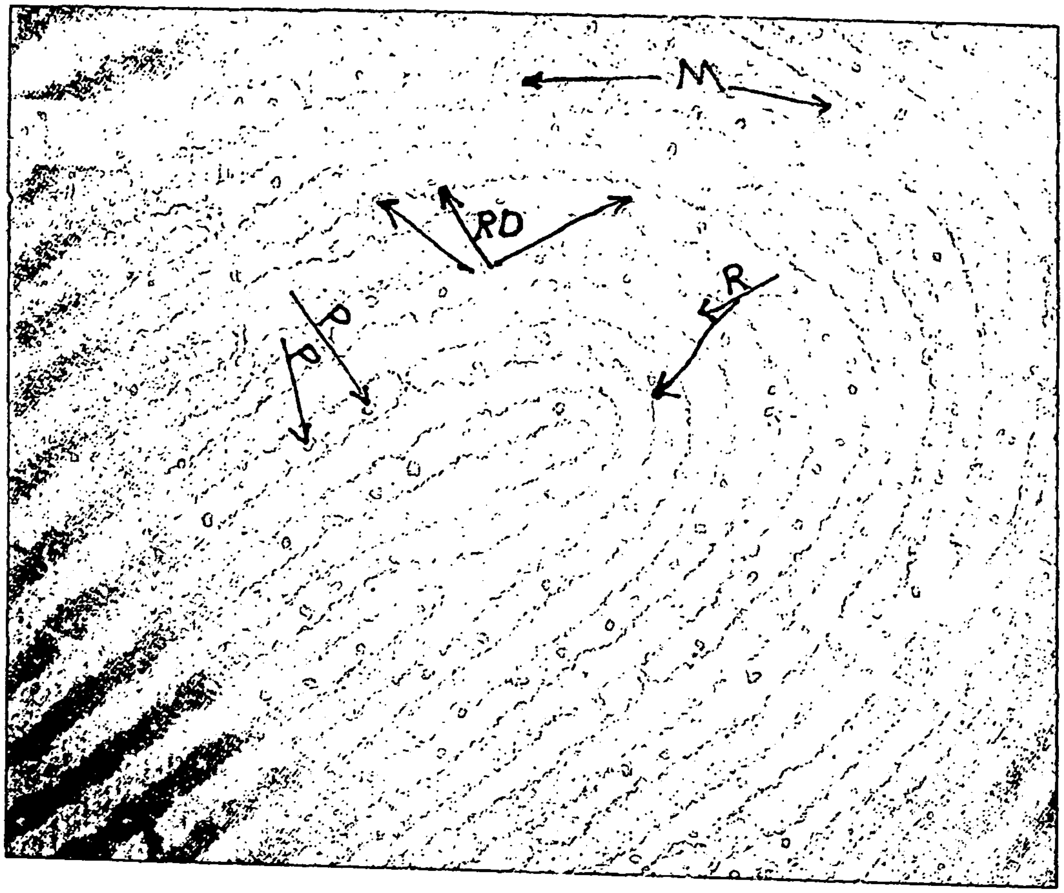

Figure 4. A fingerprint image acquired with the apparatus of Figure 2 according to the procedure outlined in Figure 3. The valleys are light, and the ridges are dark with light circular pores. The image contains less than 10 minutiae and almost 10 times as many pores as minutiae. Examples of pores, P, ridges, R, ridge details, RD, and minutiae, M, are indicated in Figure by the labeled arrows.

After acquisition an image is transferred to a local or remote networked computer by one of a number of possible connecting protocols such as IEEE 1394 (Firewire), USB, Serial ATA, or Ethernet. The image is then converted to a desired file format and header information and possibly a watermark are added to the image. The header will contain information regarding the fingerprint and how, when and where it was acquired, and pointers to related information such as personal information about the individual, including, but not limited to, a photograph, voice print and other identifying information. A watermark can be added to protect the image from subsequent unauthorized alteration. One example of a procedure to add a watermark to fingerprint images is described by Yeung and Pankanti, "Verification watermarks on fingerprint recognition and retrieval" Journal of Electronic Imaging, 9(4), 468-476(2000). Commercial watermarking procedures, such as those of Digimarc Corporation, can also be used.

Construction of Fingerprint Model

After a fingerprint is acquired specific and unique features of the print are identified, extracted and stored as a "trained model" according to the procedure shown in Figure 5. The model will be used for subsequent fingerprint verification (one to one

matching) by comparing the feature sets of the model to the corresponding features of a subject image. Features from the entire image are usually extracted and stored for fingerprints that are to be used for fingerprint identification (one to many matching)

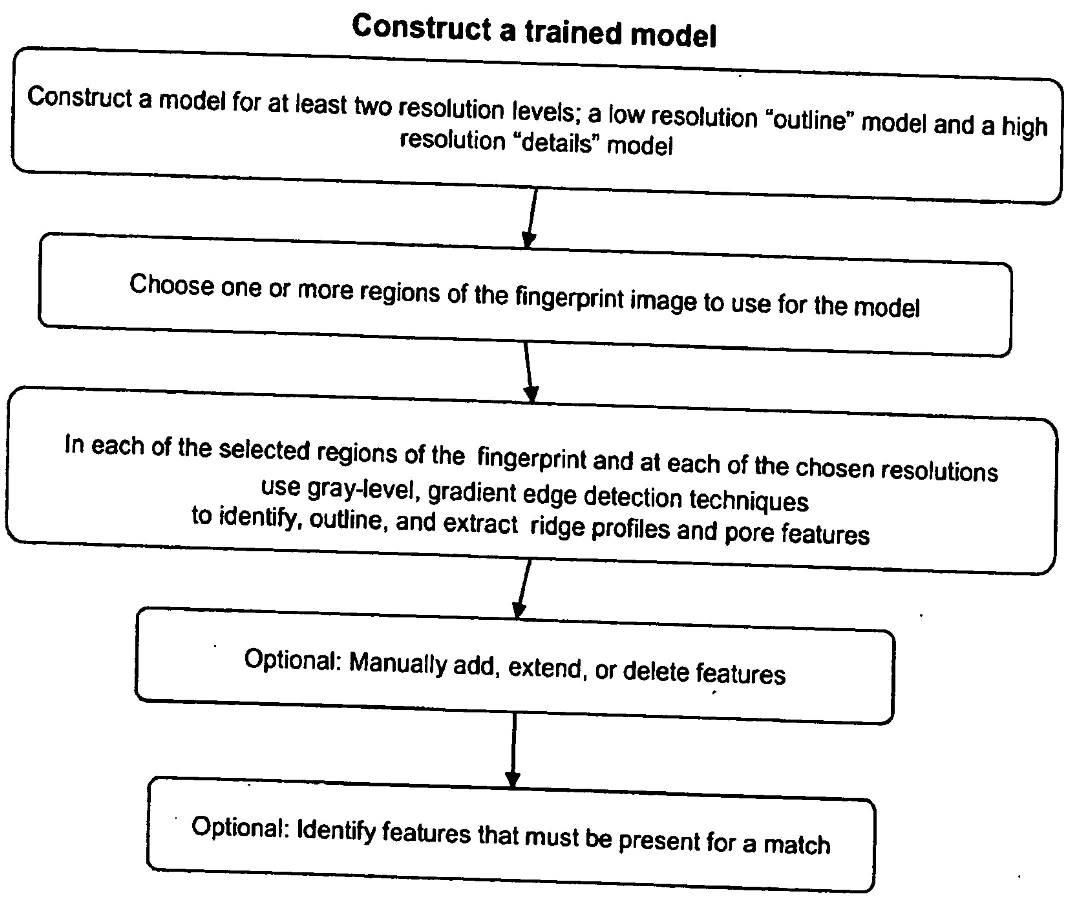

Figure 5. A flow diagram for creating a model of a fingerprint that can be used for subsequent analysis and matching.

At least two models are built from high resolution images, a low resolution "outline" model that comprises ridge contours, and a high resolution "details" model that comprises ridge contours, ridge shapes, and pores. Details regarding ridge shapes, and pores are generally not considered in the outline model; compare Figure 6 for an example of the features that are typically identified at the outline level to Figure 8 for features found at the details level. Since the outline model contains less information, computation time is reduced by first comparing images at the outline level before attempting to match images at the details level. Both outline and details models are built using the same procedure of gray-scale gradient edge detection. The outline model is determined from a subset of pixels of the original image; each pixel of the subset is an average value over a predetermined number of neighboring pixels from the original image. The first step

during fingerprint matching is to compare outline models. Matches that are discovered at the outline level are then compared at the details level.

Images acquired by the device shown in Figure 2 are 6.1 mm by 7.7 mm. This relatively large fingerprint is usually divided into one or more smaller regions that are individually used to construct a composite model. These smaller regions can either be chosen manually to capture particularly interesting features, or they can be chosen automatically using adjustable software settings that define the number of regions, region size, and locations. Their size is chosen to be large enough to include numerous characteristic features, and to be small enough to reduce problems associated with plastic deformation of the skin and to minimize computation time. The features identified in a sub region of the complete fingerprint are referred to as a feature set; a trained model comprises a collection of all of the feature sets for a particular fingerprint.

Features, for each resolution level, and in each region of the fingerprint chosen to be part of the trained model, are identified and extracted using gray-level gradient edge detection procedures. The gradient is first estimated for each of the pixels of the model using one of a relatively large number of procedures that have been developed for this process (see for example D. A. Forsyth, and J. Ponce, "Computer Vision A Modern Approach", Prentice Hall, New Jersey, 2003, chapter 8, or P. F. Whelan, and D. Molloy, "Machine Vision Algorithms in Java", Springer, London, 2000, chapter 3). A particularly useful procedure that is often used to estimate gradients is to apply a Gaussian noise filter to the image and then to perform the gradient calculation using a "finite differences" algorithm. After calculation of the gradients an image point with a locally maximal gradient in the direction of the gradient is identified and marked as an edge point. The next step is to identify neighboring edge points. This is usually accomplished by finding the nearest pixels to the original edge point that lie in a direction that is approximately perpendicular to the gradient direction that passes through the first edge point. The gradient values for these new pixels are determined, and the pixel with a gradient that is maximal along its gradient direction and has a value that exceeds a threshold is assigned to be the next edge point. This procedure is continued either until the edge is terminated or the edge closes with itself to form a continuous curve. Edge termination occurs at the previously determined edge point if the gradient of a candidate edge point is less than the threshold. In the next step a previously unvisited edge point is identified and its edge is traced according to the steps outlined above. This whole process is repeated until all of the potential edge points have been considered. Automatic software procedures are then used to distinguish fingerprint features from noise. Real edges, for example, must define features that have a minimum width. In addition, lines that do not enclose pores must extend for a minimum distance in order to be considered as legitimate feature edges. Additional rules are applied by adjusting software settings. Optional steps allow the models to be manually edited by adding or deleting features, and allow users to indicate certain features of the model that must be present for a successful match. All editing is performed on the features and not on the original image which is deliberately protected from any alteration. Examples of features that are identified by this procedure are shown in Figures 6, 7, and 8.

A number of commercial software applications can be used for edge detection, including Aphelion from Amerinex Applied Imaging, Hexsight software from Adept, Vision Blox distributed in the USA by Image Labs, and Halion from The Imaging Source.

After feature extraction to produce the trained model the original fingerprint can be compressed, encrypted, and stored. One compression procedure is the FBI standard for 500 dpi fingerprints, referred to as Wavelet/Scalar Quantization (WSQ). This is a lossy scheme with a compression ratio of 12.9. The compressed image needs to form a record of the original print that can be used for manual matching and for some automatic matching procedures. The trained model used for matching, on the other hand, requires very few bytes of storage, and can be stored without compression.

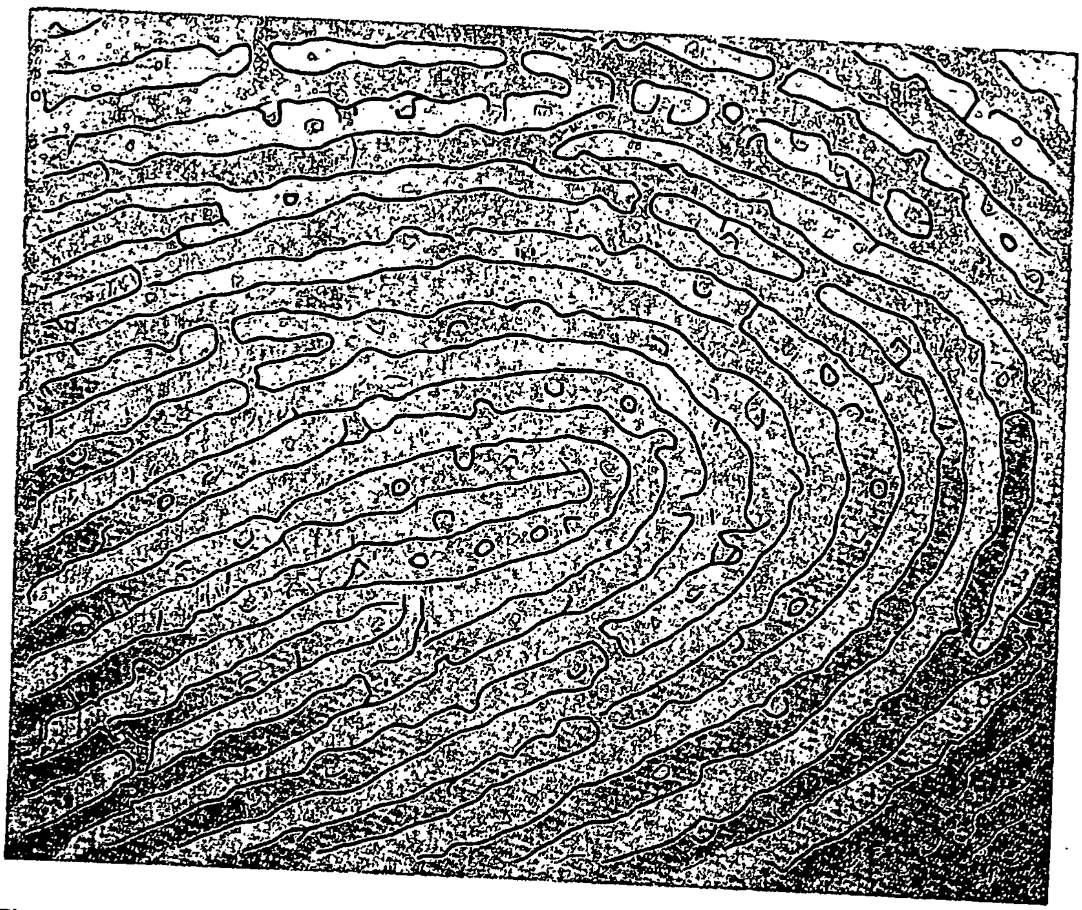

Figure 6. An example of features obtained at the "outline" resolution level. The red lines trace the ridge:valley boundaries and outline some of the pores.

Figure 7. A fingerprint with a smaller central region containing highlighted features that were identified using gray-scale gradient edge detection procedures as discussed in the text. These features were obtained at the "details" level of resolution.

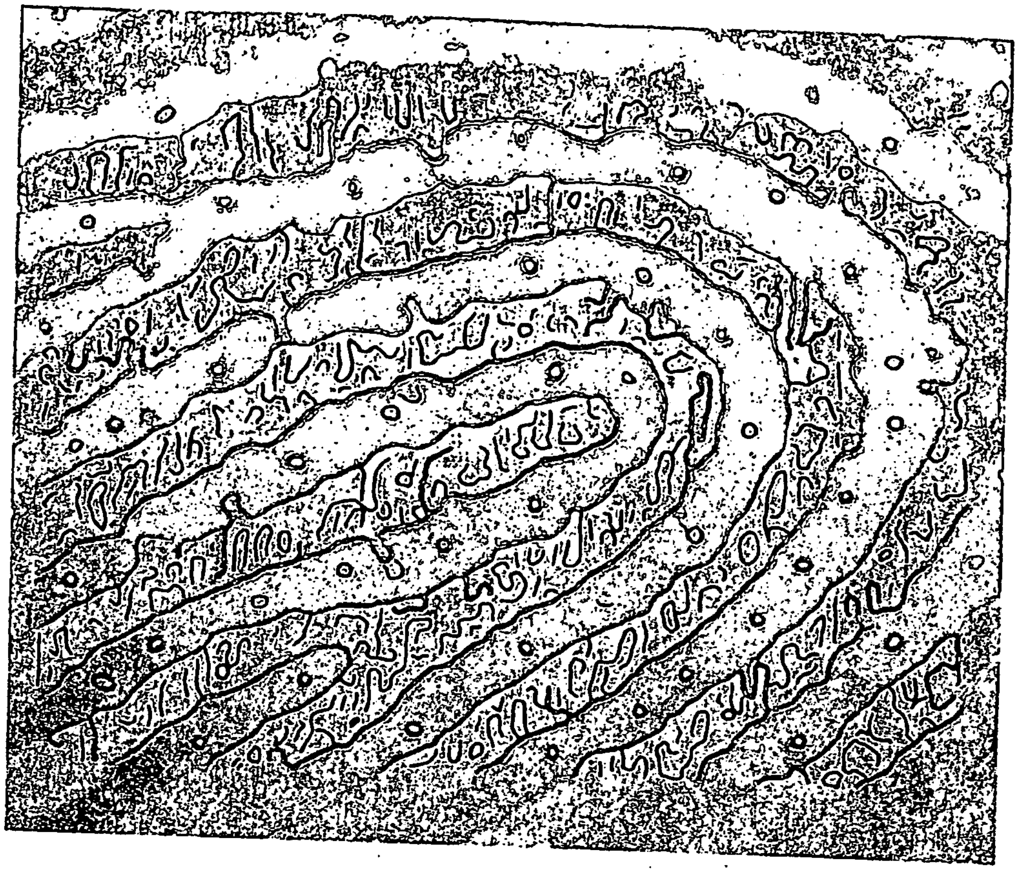

Figure 8: An expanded view of the model region from the fingerprint shown in Figure 6. Features that are outlined in green are considered real and are used for subsequent fingerprint matching steps. Noise is traced in blue and will not be used for matching. A trained model of a single fingerprint comprises one or more of these feature sets from various regions of the complete fingerprint image.

Fingerprint Matching

Fingerprint matching is used either to verify the identity of an individual, or to identify the source of an unknown fingerprint. Both procedures compare a known print from a data base to either a live scan print for verification, or to an unknown print for identification. The fundamental step of fingerprint matching is the same for both verification and identification.

Fingerprint Verification

A particularly important type of fingerprint matching compares a live scan image to an enrolled image in order to verify the identity the individual presenting the live scan fingerprint. Flow diagrams for fingerprint verification are shown in Figures 9 and 10.

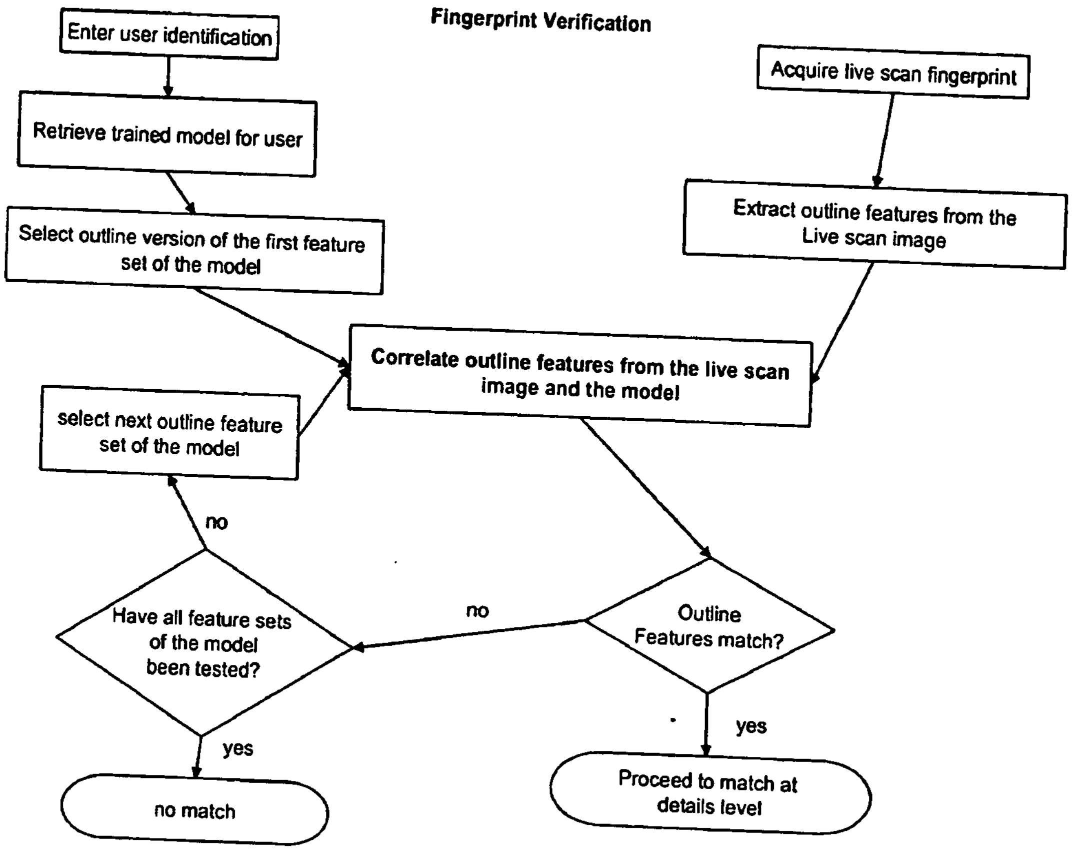

Figure 9. A flow diagram of the steps for fingerprint verification at the "outline" resolution level.

A user first presents identification such as a name or password. Then a live scan, high resolution fingerprint of the user is acquired and "outline" and "details" features for the complete print are identified according to the procedures of the present invention described above. An outline feature set from the trained model of the user is compared to the corresponding features from the live scan image. This comparison is repeated until either a match is found or all of the feature sets of the model have been compared to the live scan outline features. If a match is found at the outline level then the matching procedure is repeated at the details level according to Figure 10.

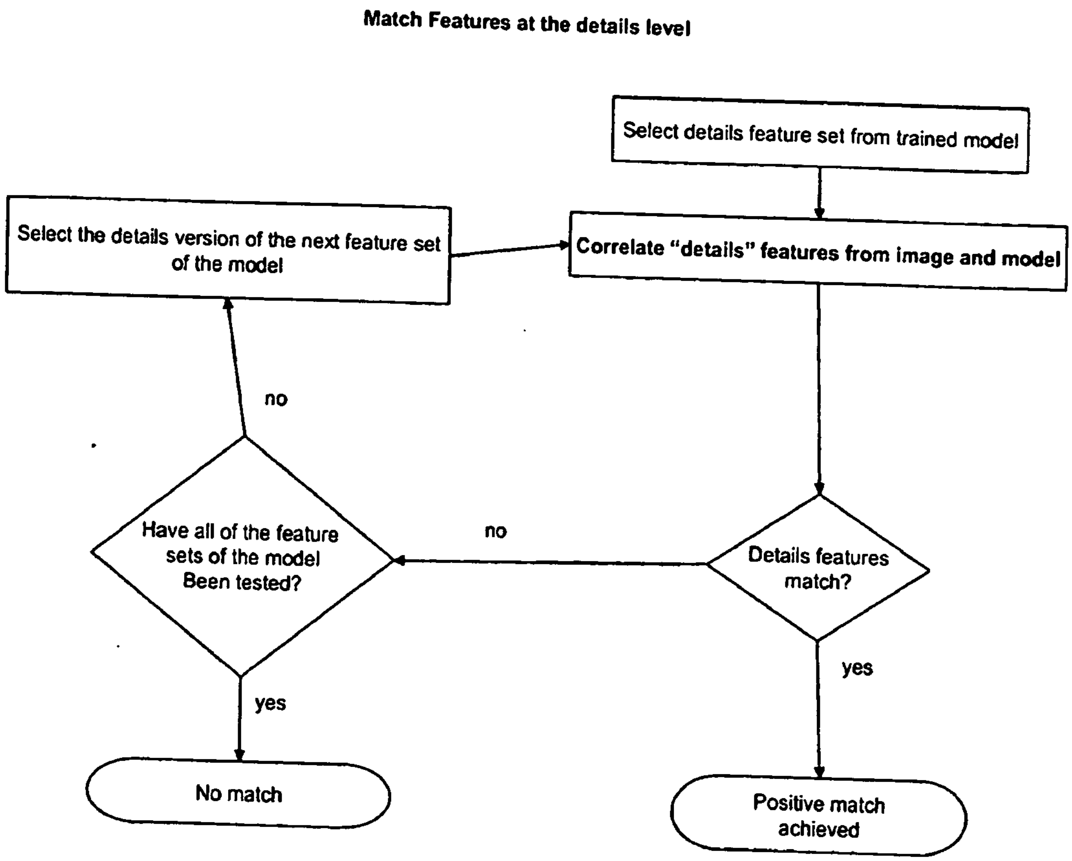

Figure 10. A flow diagram for fingerprint verification at the "details" resolution level.

Fingerprint features are correlated according to the procedure shown in Figure 11.

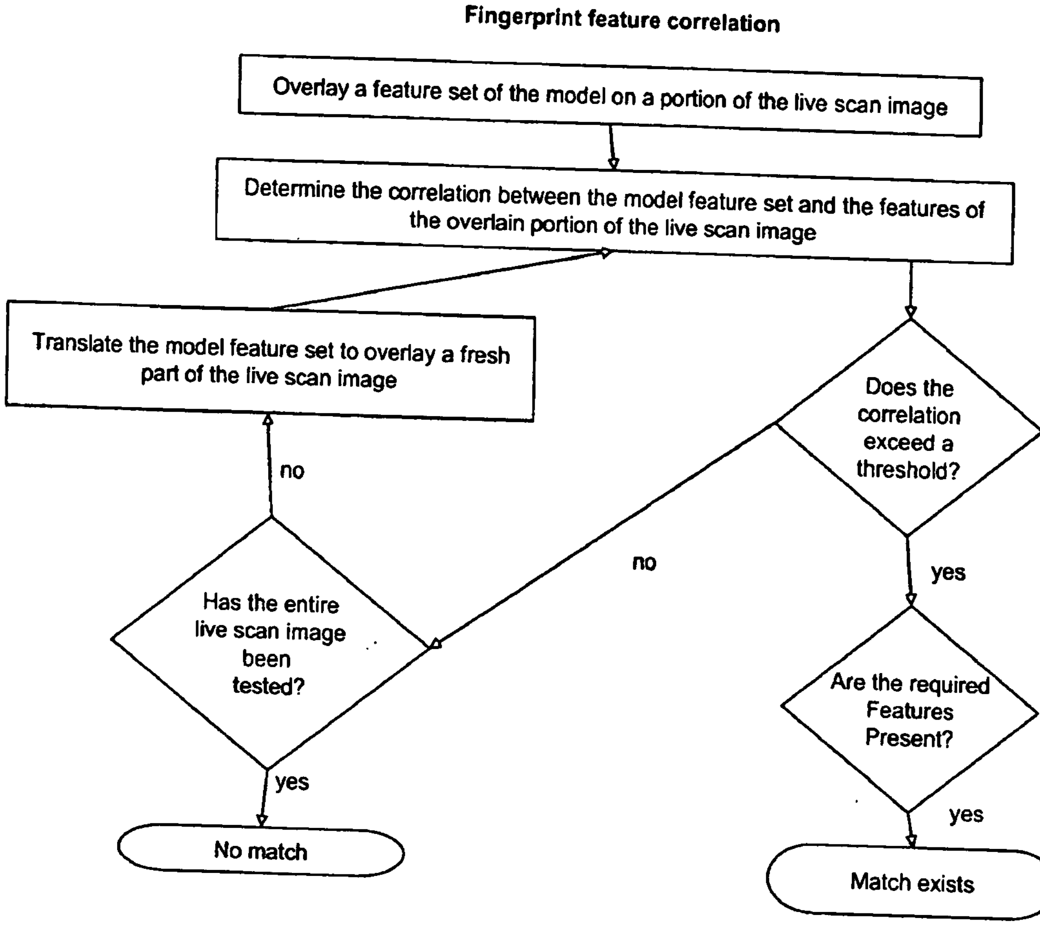

Figure 11. A flow diagram outlining the procedure used to determine if a match exists between a trained model and a live scan fingerprint.

The procedure of Figure 11 is applied for both the outline and details levels of resolution. A model feature set is overlain on a feature set of the entire live scan image. Since the model feature set is smaller it will overlap only a portion of the live scan feature set. A correlation is then calculated between the model feature set and the portion of the live scan image that it overlays. There are a number of procedures that are commonly used to determine correlation between images (for example Maltoni, Maio, Jain, and Prabhakar, "Handbook of Fingerprint Recognition", Springer, 2003, chapter 4). A particularly useful procedure considers the similarity of two images to be indicated by their "cross correlation" (for example Maltoni, Maio, Jain, and Prabhakar, "Handbook of Fingerprint Recognition", Springer, 2003, chapter 4). Using this procedure the cross correlation between the live scan image and the model feature set is calculated as the feature set expands, contracts, and rotates, over predetermined limits, with respect to the live scan image that it overlays. The feature set is then translated to a new section of the

live scan image and the cross correlation calculation is repeated. This process is followed for all the feature sets of the model. A match is achieved if a cross correlation exceeds a threshold, and if a predetermined percent of required features match with the live scan image.

Fingerprint Identification

Fingerprints from an unknown individual can sometimes be identified by comparing the unknown print to a data base of known prints. A particularly advantageous procedure is to compare prints in a data base of high resolution fingerprints that were acquired and processed according to the procedures of Figures 1, 3, and 5 with a high resolution unknown print. In this case each print in the data base would have both an associated "outlines" and "details" feature set that encompassed the entire fingerprint image. A trained model would be formed from the unknown print and compared to the feature sets of the data base. To save computation time the comparison would first be made at the "outline" resolution level. The subset of prints that matched at the outline level would subsequently be compared at the "details" resolution level.

It is also possible to compare a relatively low resolution unknown print to prints in either a high or a low resolution data base In these cases the feature set for the unknown print would comprise only ridge patterns, and would not contain information on ridge profiles, ridge shapes, or pores. Our procedure should exhibit enhanced reliability over minutiae-based systems even in this case since all of the information of the print would be used for comparison and not just a few minutiae points.

In most examples of fingerprint identification appropriate linear scaling might be necessary since the unknown fingerprint may have been acquired at a different magnification from the fingerprints in the comparison data base.